



CHIEF  
COMMUNICATIONS AND LIAISON

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224

JUN 2 2003

MEMORANDUM FOR Richard Stone, Acting Director  
Mission Assurance  
M:S:A  
FROM: *Mary J. Ronan Jr.*  
Mary Ronan  
Acting Privacy Advocate CL:PA  
SUBJECT: Sensitive Systems Database  
Privacy Impact Assessment (PIA)

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment for the Sensitive Systems Database. Based on the information you provided, we do not have any privacy concerns that would preclude this system from operating. However, a revised PIA is required when considering any future upgrades or modifications to the system.

We will forward a copy of the PIA to the Information Technology Services Security and Certification Program Office to be included in the Security Accreditation Package for formal acceptance for operation. The Office of Security Evaluation and Oversight, which has security oversight responsibility, may request information concerning the statements contained in the PIA to ascertain compliance with applicable requirements.

If you have any questions, please contact me at 202-622-9474 or Priscilla Hopkins at 202-927-9758.

Attachment


cc: Director, Information Technology Services Security and Certification  
Program Office M:S:C:C  
Director, Office of Security Evaluation and Oversight M:S:S



DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224

APR 30 2003

MEMORANDUM FOR CHARLENE W. THOMAS  
ACTING PRIVACY ADVOCATE CL:PA

FROM:  Richard A. Stone, Acting Director, Mission Assurance M:S:A

SUBJECT: Request for Privacy Impact Assessment (PIA) –  
Sensitive Systems DataBase (SSDb)

Purpose of the System: The Sensitive Systems Database (SSDb) is a Microsoft Access 2000 database, which allows for data entry of systems/applications, which require monitoring to ensure that the appropriate security activities, such as certification, are performed in a timely fashion. The automated tracking system will allow the user (Certification Program Office Analysts/Management only) to select information from the database based on criteria entered by the user. The program will also generate a variety of output reports, any of which can be sent to a printer or to a file on the analyst's computer. This tracking system helps the section by reducing time necessary to manually sort information in the inventory. Reports generated will be used to notify management of the status, on a regular basis, of all tracked activities for any given system in the database.

Name of Request Contact:

Name: Mike Morrison

Organization Name & Symbols: Certification Program Office M:S:A:C

Mailing Address: 5000 Ellin Road Lanham, MD 20706

Phone Number (with area code): 202-283-6620

Name of Business System Owner:

Name: Richard Stone

Organization Name & Symbols: Mission Assurance M:S:A

Mailing Address: 5000 Ellin Road Lanham, MD 20706

Phone Number (with area code): 202-283-4806

Requested Operational Date: May 30, 2003

Category: (Reason PIA is required--enter "y" or "n" and applicable dates)

New System?: Y

Recertification? (if no change, enter date of last certification) N

Modification of existing system?: N

Is this a National Standard Application (NSA)?   N  

Is this a Modernization Project or System?   N  

If yes, the current milestone?:        (Enter 1-5; explain if combining milestones)

System of Record Number(s) (SORN) #: (coordination is required with Office of Disclosure--contact David Silverman, 202-622-3607) The SSDb is covered by the Treasury/IRS 34.037, IRS Audit Trail and Security Records System.

Attachment: PIA

## Data in the System

<p>1. Describe the information (data elements and fields) available in the system in the following categories:</p> <p>A. Taxpayer B. Employee C. Audit Trail Information (including employee log-in info) D. Other (Describe)</p>	<p>A. None. B. Employee Names, Organizational Symbols, Business Phone Numbers. C. None. D. None.</p>
<p>2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.</p> <p>A. IRS B. Taxpayer C. Employee D. Other Federal Agencies (List agency) E. State and Local Agencies (List agency) F. Other third party sources (Describe)</p>	<p>A. None. B. None. C. The System Administrator enters all values directly into the SSDb. D. None. E. None. F. None.</p>
<p>3. Is each data item required for the business purpose of the system? Explain.</p>	<p>Yes. The information in the SSDb is required so that management can monitor certification activities, track inventory of IRS systems certification, and generate reports to notify management of IRS system certification status.</p>
<p>4. How will each data item be verified for accuracy, timeliness, and completeness?</p>	<p>Certification Analysts complete a form with all system owner and point of contact information which is then sent to the System Administrator for data entry.</p>
<p>5. Is there another source for the data? Explain how that source is or is not used.</p>	<p>No.</p>

6. Generally, how will data be retrieved by the user?	Data will be retrieved via entry screen displays and system generated reports. Only the System Administrator and Certification Analysts in the Certification Program Office have access to the SSDb.
7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?	Yes. Queries can be performed to retrieve data by System Name or Employee Name (Certification Analyst, System Owner Point of Contact Information).

### Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?	Only the System Administrator and staff members/managers in the Certification Program Office have access to the SSDb.
9. How is access to the data by a user determined and by whom?	Only the System Administrator and staff members/managers in the Certification Program Office have access to the SSDb. Access is provided by the System Administrator.
10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared. If NO, continue to Question 12.	No.
11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?	Not Applicable.
12. Will other agencies provide, receive, or share data in any form with this system?	No.

### Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?	The data is never eliminated from the SSDb. All data is kept for history purposes and certification status.
14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.	No.
15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.	The SSDb tracks the certification status of IRS systems along with the point of contact information and certification analyst assigned.
16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.	No.
17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.	No.
18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?	The SSDb is not designed to collect negative determinations.
19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?	No.